UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,161	06/25/2003	Sylvie Wuidart	00RO36654290	5008

27975 7590 11/09/2006

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/606,161	WUIDART, SYLVIE	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *11-22* is/are allowed.

6)☒ Claim(s) *1,5-7,10,23,24,28,29,31 and 32* is/are rejected.

7)☒ Claim(s) *2-4,8,9,25-27 and 30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/25/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The IDS of 6/25/2003 was received and considered.

2. Claims 1-32 are pending.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 31 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 31, the limitations "the first logic function" (line 3) and "the second logic function" (line 3) lack sufficient antecedent basis. *For the purposes of this Office Action, claim 31 is understood to depend from claim 28.*

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 5, 10, 23-24 & 32 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,839,847 to Ohki et al. (**Ohki**).

Regarding claim 1, Ohki discloses a logic circuit for performing a logic function (Fig. 1), and having N data inputs (64-bit plain text and cipher key of 56-bits) and M data outputs (64-bit ciphertext output) (col. 6, lines 41-48), N being at least equal to 2 and M being at least equal to 1, the logic circuit comprising at least one logic gate/circuit for performing the logic function (col. 8, lines 1-14) in at least two different ways (depending on random signal, repetition unit repeats processing) (col. 8, lines 42-60), the way in which the logic function is performed being based upon a value of a function selection signal (col. 8, lines 55-60) such that for identical data received at the N data inputs and for different values of the function selection signal, at least one of polarities of certain internal nodes of the logic circuit are not identical (col. 8, lines 43-49) and current consumption of the logic circuit is not identical (col. 8, lines 58-60). Not that while the random signal affects repeat processing, identical results are accomplished regarding the output/result of the encryption processing.

Regarding claims 5 & 32, Ohki discloses the selection signal being generated randomly (col. 8, lines 6-14 & lines 43-50).

Regarding claim 10, Ohki discloses an encryption function (col. 6, lines 41-48).

Regarding claim 23, Ohki discloses a method for scrambling operation of a logic circuit that performs a logic function (Fig. 1), the logic circuit having N data inputs (64-bit plain text and cipher key of 56-bits) and M data outputs (64-bit ciphertext output) (col. 6, lines 41-48), N being at least equal to 2 and M being at least equal to 1, the method comprising performing the

logic function (col. 8, lines 1-14) in at least two different ways (depending on random signal, repetition either repeats processing or continues with normal processing) (col. 8, lines 42-60) using at least one logic gate/circuit (col. 8, lines 1-14), the way in which the logic function is performed being determined by a value of a function selection signal (col. 8, lines 55-60) such that for identical data received at the N data inputs and for different values of the function selection signal, at least one of polarities of certain internal nodes of the logic circuit are not identical (col. 8, lines 43-49) and current consumption of the logic circuit is not identical (col. 8, lines 58-60) and refreshing the function selection signal at predetermined instants so that the operation of the logic circuit is scrambled (depending on the random signal, the logic repeats processing) (col. 8, lines 42-60). Not that while the random signal affects repeat processing, identical results are accomplished regarding the output/result of the encryption processing.

Regarding claim 24, Ohki discloses the function selection signal being randomly applied to at least one logic gate/circuit (col. 8, lines 1-14).

7. Claim 1 is rejected under 35 U.S.C. 102(a) as being anticipated by MC14001B Series CMOS gates, described in "MC14001B Series B-Suffix Series CMOS Gates" by ON Semiconductor (**ON**).

Regarding claim 1, ON discloses a logic circuit/MC14025B Triple 3-Input NOR gate for performing a logic function/NOR, and having N/2 data inputs and M/1 data outputs, N being at least equal to 2 and M being at least equal to 1 (p. 2), the logic circuit comprising at least one logic gate for performing the logic function/NOR (p. 2) in at least two different ways (see table below, for example pin 1 high versus pin 1 low), the way in which the logic function is

performed being based upon a value of a function selection signal/pin 1 (p. 2) such that for identical data received at the N data inputs (pins 2 and 8) and for different values of the function selection signal (pin 1), at least one of polarities of certain internal nodes of the logic circuit are not identical and current consumption of the logic circuit is not identical (see table and explanation below). As per the table below, and by the definition of the gate shown, if the function selection signal is a logic "0", an input of Pin 2 = "0" and Pin 3 = "0" yields an output Pin 9 = "1". Upon a different value of the function selection signal, Pin 1 = "1" with the identical inputs, the output, Pin 9 = "0". Therefore, the polarities of internal nodes of the circuit are not identical. Further, current consumption of the logic circuit is not identical (see table "Electrical Characteristics" on p. 3, where for a reference voltage constant, the output current is, for example, -3mA for a high output and the output current is 0.64mA.

Pin 1 (function selection)	Pin 2 (input 1)	Pin 3 (input 2)	Pin 9 (output)
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

8. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by the Quad 2-Line to 1-Line Data Selectors/Multiplexers, described in "Quad 2-Line to 1-Line Data Selectors/Multiplexers" by National Semiconductor (**NS**).

Regarding claim 1, NS discloses a logic circuit (p. 1) for performing a logic function/multiplexing (p. 1), and having at least N/2 data inputs and M/1 data outputs, N being at least equal to 2 and M being at least equal to 1 (p. 1), the logic circuit comprising at least one logic gate (p. 4) for performing the logic function in at least two different ways (see "Function Table", p. 1 and elaboration of same described below), the way in which the logic function is performed being based upon a value of a function selection signal/SELECT (p. 4) such that for identical data received at the N data inputs and for different values of the function selection signal/SELECT, at least one of polarities of certain internal nodes of the logic circuit are not identical and current consumption of the logic circuit is not identical (see "Function Table", p. 1 and elaboration of same described below). For SELECT = "0", Y=A and for SELECT = "1", Y=B. Therefore, as per the highlighted areas of the table below, corresponding to the Function Table on p. 1 of NS, with identical data inputs, but different function selection signals, the output polarities are different. Further, for high or low output Y, current consumption is –0.4mA and 4mA, respectively.

SELECT	A	B	Output Y
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1

1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 6-7 & 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ohki**, as applied to claim 1 above, in further view of U.S. Patent 4,968,903 to Smith et al. (**Smith**).

Regarding claim 6, Ohki lacks a first group of transistors, a second group of transistors and function selection means for validating one of the first and second logic functions at the output of said at least one logic gate based upon the value of the function selection signal. However, Smith teaches a first group of transistors performing a first logic function and a second group of transistors performing a second logic function (Fig. 3) and a function selection means/configuration input (col. 3, line 60 – col. 4, line 7) connected to said first and second groups of transistors (Fig. 3) and having an input (input terminal to transistor 28) for receiving a function selection signal for validating one of the first and second logic functions at the output of said at least one logic gate based upon the value of the function selection signal (col. 3, line 60 –

col. 4, line 7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Ohki to include the multi-function logic circuit of Smith for the repetition operations. One of ordinary skill in the art would have been motivated to perform such a modification to reduce the complexity of and the need for duplicate circuitry, as taught by Smith (Fig. 3 & col. 3, line 60 – col. 4, line 7) and to maintain the state of the "real" calculations when performing repeated operations that are redundant.

Regarding claim 7, Ohki, as modified above by Smith, teaches wherein said first group of transistors comprises first (Smith, Fig. 3, #28) and second stages (Smith, Fig. 3, #22-26) of transistors and said second group of transistors comprises first (Smith, Fig. 3, #29) and second (Smith, Fig. 3, #22-25) stages of transistors and wherein said function selection means/XOR comprises at least on first selection transistor (Smith, Fig. 3, ##28-29) for short-circuiting the first stages of transistors based upon the value of the function selection signal (Fig. 3 & co.. 3, lines 42-67).

Regarding claims 28-29, the claims are substantially equivalent to claims 6-7. Therefore, claims 28-29 are rejected under similar rationale.

Allowable Subject Matter

11. Claims 2-4, 8-9, 11-22, 25-27 & 30-31 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. Review of the most pertinent art to the claims:

b. U.S. Patent 6,498,404 to Thuringer et al. describes reversing means/inverter for reversing the data applied to N inputs (Fig. 2, ##6-7), such that a complementary signal is created and hence complementary power consumption is affected. However, while it is inherent that a function selection signal/clock exists in the circuit, Thuringer lacks reversing the output delivered by the gate and lacks the elements of the independent claims in the instant case.

c. U.S. Patent 6,349,318 to Vanstone et al. is cited for teaching supplying a function selection signal (Figs. 1 or 3, #10 & col. 3, lines 3-5) to select a function of an encryption circuit that performs encryption in two different ways (col. 3, lines 3-5). However, the function selection signal is not randomly supplied and the logic function performed (ALU function) is not the same function (the unit 34 performs the function over a finite field and the unit 36 performs the function over integers). The same input, with the exception of the function selection signal (signal 10 in Figs. 1 and 3), would not yield the same output and hence the function is not the same.

d. U.S. Patent 4,968,903 to Smith et al. describes a circuit performing two different logic functions based on a selector signal (see, for example, Fig. 4).

13. However, the following reasons for allowance are given regarding the claims.

e. Regarding claim 2, the prior art relied upon fails to teach or suggest reversing means (inverting) for reversing the data applied to the N inputs of said at least one logic gate, and for reversing the data delivered by said at least one logic gate based upon the

value of a function selection signal, in combination with the limitations of the parent claim.

f. Regarding claim 3, the claim is allowable due to its dependence upon claim 2.

g. Regarding claim 4, the prior art relied upon fails to teach or suggest a logic gate comprising a plurality of logic gates for performing a NAND logic function when a function selection signal has a first logic value and for performing a NOR logic function when the function selection signal has a second logic value, in combination with the limitations of the parent claim.

h. Regarding claim 8, the prior art relied upon fails to teach or suggest a function selection means comprising at least one second selection transistor for interrupting conductive paths in second stages of transistors based upon the value of a function selection signal, in combination with the limitations of the parent claim.

i. Regarding claim 9, the prior art relied upon fails to teach or suggest a logic circuit comprising a first group of transistors for performing a first logic function and a second group of transistors for performing a second logic function, wherein the first logic function is a NAND logic function and the second logic function is a NOR logic function, in combination with the limitations of the parent claim.

j. Regarding claim 11, the prior art teaches performing a logic function (encryption) in a circuit in two different ways (with unnecessary repetition and without, see Ohki reference), but the prior art relied upon fails to teach or suggest a secured integrated circuit with the feature of an encryption circuit comprising a plurality of encryption blocks, each encryption block for performing a logic function in at least two different

ways, the way in which the logic function is performed being based upon a value of a function selection signal and a random signal generator connected to said plurality of encryption blocks for randomly providing the function selection signal to each encryption block, in combination with the remaining limitations of the claim.

k. Regarding claims 12-22, the claims are allowable based on their dependency upon claim 11.

l. Regarding claim 25, the prior art relied upon fails to teach or suggest reversing (inverting) the data applied to the N inputs based upon the value of a function selection signal and reversing the data delivered by the at least one logic gate based upon the value of the function selection signal, in combination with the limitations of the parent claim.

m. Regarding claim 26, the claim is allowable due to its dependence upon claim 25.

n. Regarding claim 27, the prior art relied upon fails to teach or suggest where the at least one logic gate, performing a logic function in at least two different ways, comprises a plurality of logic gates for performing a NAND logic function when the function selection signal has a first logic value and for performing a NOR logic function when the function selection signal has a second logic value, in combination with the limitations of the parent claim. Regarding claim 28, the claim is allowable due to its dependence upon claim 26.

o. Regarding claim 30, the prior art relied upon fails to teach or suggest a function selection circuit comprising at least one second selection transistor for interrupting conductive paths in the second stages of transistors based upon the value of the function selection signal, in combination with the limitations of the parent claim.

p. Regarding claim 31, as best understood, the prior art relied upon fails to teach or suggest a logic circuit comprising a first group of transistors for performing a first logic function and a second group of transistors for performing a second logic function, wherein the first logic function is a NAND logic function and the second logic function is a NOR logic function, in combination with the limitations of the parent claim.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

q. U.S. Patent 6,658,569 to Patarin et al. is cited for teaching splitting the inputs into multiple blocks and operating on those blocks separately by an encryption circuit. The blocks are reconstructed to create the finished product. The purpose of this is to randomize the power requirements of the circuit as a whole (col. 3, lines 1-8, col. 4, lines 15-25 & Fig. 2).

r. U.S. Patent 6,804,782 to Qui et al. is cited for teaching that to randomize power usage in a cryptographic circuit, unnecessary mathematical operations are performed and/or unnecessary storage of data is performed (col. 1, lines 45-65).

s. U.S. Patent Application Publication 2002/0124178 to Kocher et al. is cited for teaching the introduction of random noise modules of any type, but not performing explicitly the same functions (¶¶34-40).

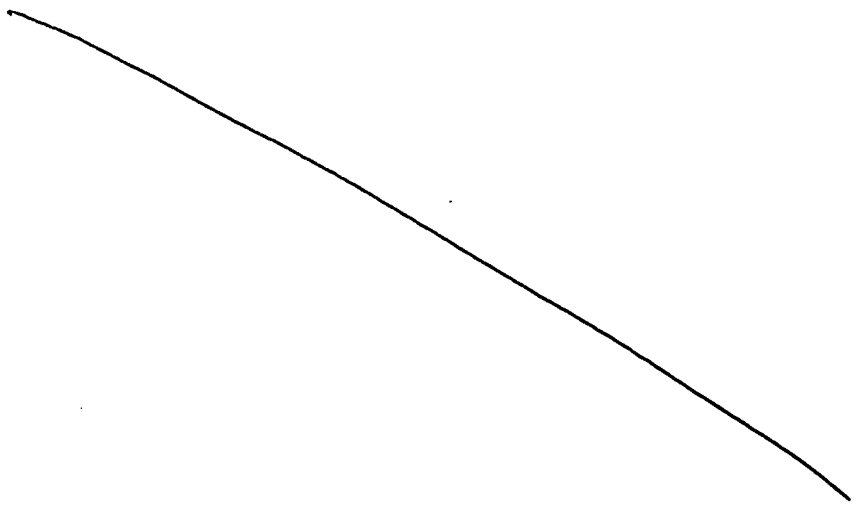
t. U.S. Patent 6,419,159 to Odinak is cited for teaching randomly turning on and off individual ground sinks to randomly change power requirements (abstract).

u. U.S. Patent 6,654,884 to Jaffe et al. is cited for teaching that a single logic function can be performed in at least two different ways (col. 9, lines 35-43), such as for instance an inversion can be performed using a NOT gate or a NAND gate. Further, one of ordinary skill in the art knows that these many gates would use different currents and polarities. However, Jaffe does not describe selecting between two circuits that perform the same function.

v. Computer Organization and Design, The Hardware/Software Interface by Hennessy et al. is cited for teaching, among other important concepts, DeMorgan's Theorems. These at least state that a certain logic function can be performed using more than one logic configuration (pp. B2-B11 & B46).

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

October 18, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100